UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

IN RE: CAPITAL ONE CONSUMER DATA SECURITY BREACH LITIGATION	)	MDL No. 1:19md2915 (AJT/JFA)

This Document Relates to the Consumer Cases

MEMORANDUM IN SUPPORT OF PLAINTIFFS' MOTION TO COMPEL PRODUCTION OF MANDIANT REPORT AND RELATED MATERIALS

Plaintiffs submit this Memorandum in Support of their Motion to Compel Production of the Mandiant Report and Related Materials.

PRELIMINARY STATEMENT

On July 29, 2019, Capital One announced it had experienced a data breach that affected over 100 million people in the United States and six million people in Canada (the "Data Breach"). Representative Consumer Class Action Complaint ("Complaint" or "Compl."), Dkt. 354, at ¶¶ 1-2. Shockingly, however, the Data Breach had actually occurred four months earlier, in March 2019, when a hacker infiltrated Capital One's cloud network and downloaded 1.75 terabytes of extremely sensitive customer data without detection. Compl. ¶¶ 74-78.

Four years earlier, as part of its [redacted] Capital One [redacted] Capital One [redacted] *See* Ex. 1, Master Services Agreement ([redacted]), CAPITALONE_MDL_000258941, at -258941; Ex. 2, Statement of Work [redacted]), CAPITALONE_MDL_000097222, at -97223; Ex. 3,

CAPITALONE_MDL_000185309, at -185319 ([redacted]). [redacted] Mandiant responded to Capital One's Data Breach, investigated the breach, and produced – [redacted] – a final forensic report detailing its findings and recommendations (the "Mandiant Report"). *See* Ex. 2, Statement of Work, at Section 2.1 (detailing [redacted]).

Despite the fact that Mandiant [redacted] Capital One has consistently contended in multiple meet and confers over many months since January 2020 that Mandiant's investigation and its final report are privileged. *See* Dkt. 271, Capital One Defendants' Report Pursuant to Paragraph 10 at 3-4; Dkt. 269, Plaintiffs' Report Pursuant to Paragraph 10(d) at 2-3. According to Capital One, because Capital One's lawyers at Debovoise and Plimpton ("Debovoise") hired Mandiant after the Data Breach to provide [redacted] Mandiant's factual forensic findings and remediation recommendations are cloaked in privilege.

This ham-fisted attempt at claiming privilege over a business function [redacted] should be rejected. Mandiant's investigation and resulting report simply do not qualify as work product, nor as attorney-client privileged, because the key facts and documents produced to-date show Mandiant was retained for business – not litigation – purposes. In fact, in a data breach case in this District several months ago, Judge Nachmanoff ordered the production of a Mandiant Report and related materials under almost identical circumstances. *In*

re: Dominion Dental Servs. USA, Inc. Data Breach Litig., No. 1:19-CV-1050-LMB-MSN, 2019 WL 7592343, at *3 (E.D. Va. Dec. 19, 2019).

[redacted] the defendant in *Dominion* executed a statement of work with Mandiant *before* discovering the data breach at issue in the litigation. *Id.* at *1. [redacted] that statement of work included incident response in the event of a breach and deliverables, including an incident response report. *Id.* Even though the existing statement of work was still in place when the breach was discovered, the defendant's outside counsel executed a second, replacement statement of work with Mandiant purportedly sweeping the services Mandiant was already engaged to conduct under their purview, and then claimed privilege over the investigation and attendant report. *Id.* at *2. The Court overruled the defendant's assertion of privilege. *Id.* at *3. It found that Mandiant was retained for business, not litigation, purposes, and the "'change of supervision' to outside counsel '[was] not sufficient to render all of the later communications and underlying documents privileged or immune from discovery as work product.'" *Id.* at *4 (q*uoting In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 296 F. Supp. 3d 1230, 1245 (D. Or. 2017) (also ordering production of Mandiant Report under similar circumstances)).

For these same reasons, the Court should find the Mandiant Report here is not privileged. Facts are not protected from disclosure and the investigation was a necessary business function; having an attorney oversee the factual investigation does not grant it special protection. Indeed, Mandiant's report is not privileged because it contains *facts* – not legal advice and conclusions – about the who, what, where, when, and how of the breach.[1] Even if Capital One's counsel may use the report and its conclusions to assist them in giving legal advice to their client, that does not

[1] If the court is disinclined to order the Mandiant Report to be produced, it should undertake an *in camera* review to see the true nature of the types of information contained in this report.

protect the facts contained therein from discovery. Any company that is the target of a data breach must undergo a similar assessment for business purposes and to ensure customers and regulators that it has uncovered and remedied the breach, regardless of whether it is ultimately sued in litigation. Thus, these legitimate business purposes for the retention of Mandiant obviate any claims that Mandiant was engaged solely to provide legal advice.

However, even if the Court finds that the Mandiant investigation and report are privileged, Capital One should still be compelled to produce the Report and requested materials for two reasons. *First*, Capital One has waived the privilege over the report by disclosing the report and its conclusions to third parties. *Second*, the Report is critical to Plaintiffs' investigation and prosecution of this case and Plaintiffs have no other reasonable way to obtain the detailed forensic information and remediation recommendations contained in the highly technical Mandiant Report. Given the limited period of time afforded the parties to conduct discovery, Plaintiffs do not have the ability to retrace the steps already taken by Mandiant to determine the cause and scope of the data breach or to determine the necessary remediation to prevent further exposure. In addition, Plaintiffs are entitled to know, for example, what Mandiant told Capital One it was required to fix in order to ensure that its data security flaws were resolved to determine whether Capital One has actually complied with those recommendations and whether additional steps are necessary to protect the class.

In light of the arguments detailed herein, the Court should find that Mandiant's report is not privileged or work product (or that any privilege has been waived), and order Capital One to produce the report and all discoverable communications regarding the report and Mandiant's investigation. Specifically, Plaintiffs seek (1) the report and any versions thereof; (2) communications between Mandiant and Capital One employees regarding its factual conclusions

and remediation; and (3) communications between Capital One employees discussing the Mandiant report, its conclusions, and recommended remediation measures. Plaintiffs do not seek counsel's analysis of the Mandiant report, counsel's communications with Mandiant to understand the report, or counsel's direct communications with Capital One regarding the Mandiant report. Plaintiffs do, however, seek all internal Capital One communications discussing the Mandiant report and its recommendations in which counsel is merely cc'd or bcc'd in an email chain that does not contain requests for or the provision of legal advice.

LEGAL STANDARDS

A. Work Product Doctrine

Federal Rule of Civil Procedure 26(b)(3) governs the application of the work-product doctrine and federal law applies, even where jurisdiction relies on diversity.[2] Fed. R. Civ. P. 26(b)(3); *see also Chambers v. Allstate Ins. Co.*, 206 F.R.D. 579, 584 (S.D. W. Va. 2002). Rule 26(b)(3)(A) provides: "Ordinarily, a party may not discover documents and tangible things that are prepared in anticipation of litigation or for trial by or for another party or its representative."

"Courts disfavor assertions of evidentiary privilege because they shield evidence from the truth-seeking process." *RLI Ins. Co. v. Conseco, Inc.*, 477 F. Supp. 2d 741, 748 (E.D. Va. 2007) (citing *Herbert v. Lando*, 441 U.S. 153, 175 (1979); *In re Grand Jury Proceedings*, 727 F.2d 1352, 1355 (4th Cir. 1984)). Therefore, the party "claiming the protection bears the burden of demonstrating the applicability of the work product doctrine." *Solis v. Food Employers Labor Relations Ass'n*, 644 F.3d 221, 232 (4th Cir. 2011).

[2] Even if Virginia law applied, the law is the same. *See Wilson v. Norfolk & Portsmouth Belt Line R. Co.*, 69 Va. Cir. 153, 2015 WL 2650931, at *14 (2005).

Prepared "in anticipated of litigation" is key to the privilege inquiry. The Fourth Circuit applies the "because of" test to determine whether a document was created in anticipation of litigation, adopting this test in *Nat'l Union Fire Insurance v. Murray Sheet Metal*, 967 F.2d 980, 984 (4th Cir. 1992). There, it recognized that "because litigation is an ever-present possibility in American life, it is more often the case than not that events are documented with the general possibility of litigation in mind. Yet, '[t]he mere fact that litigation does eventually ensue does not, by itself, cloak materials' with work product immunity." *Id.* at 984 (quoting *Binks Mfg. Co. v. Nat'l Presto Indus., Inc.*, 709 F.2d 1109, 1118 (7th Cir. 1983)).

Instead, to qualify as work product, "the document must be prepared *because* of the prospect of litigation when the preparer faces an actual claim or a potential claim following an actual event or series of events that reasonably could result in litigation. . . . [M]aterials prepared in the ordinary course of business or pursuant to regulatory requirements or for other non-litigation purposes are not documents prepared in anticipation of litigation within the meaning of Rule 26(b)(3)." *Id.* (emphasis in original); *accord In re Grand Jury Proceedings*, 102 F.3d 748, 752 (4th Cir. 1996) (internal report documenting bank's investigation of whether bank had committed a crime, which was prepared by non-lawyer bank employee, not subject to work product doctrine).

Because there may be dual motives underlying the preparation of a particular document – one related to the prospect of litigation and one related to a business or other non-litigation purpose – the court must determine "the driving force behind the preparation of" the requested documents. *Nat'l Union Fire Ins.*, 967 F.2d at 984 (recognizing that after an accident, personnel might investigate "not only out of concern for future litigation, but also to prevent reoccurrences . . . and to respond to regulatory obligations").

The principal inquiry is whether the document would have been created in essentially the same form in the absence of litigation, or the converse, whether the document "would not have been prepared in substantially similar form *but for* the prospect of that litigation." *RLI Ins.*, 477 F. Supp. 2d at 748 (quoting *United States v. Adlman*, 134 F.3d 1194, 1195 (2d Cir. 1998)) (emphasis in original). The "because of" test requires a "case-by-case" analysis, and courts eschew bright line rules based on the timing of the document's creation or other factors. *See Westfield Ins. Co. v. Carpenter Reclamation, Inc.*, 301 F.R.D. 235, 250 (S.D. W. Va. 2014). Instead, courts consider the facts and circumstances under which the documents were created, the purpose and intent of the person creating them, and based on *in camera* examination of the documents themselves. *Id.*

Further, work product protection can be waived. In addition to public disclosure of the document or information contained therein, "when a party reveals part of a privileged communication to gain an advantage in litigation, the party waives the . . . privilege as to all other communications relating to the same subject matter. Selective disclosure for tactical purposes waives the privilege." *United States v. Jones*, 696 F.2d 1069, 1072 (4th Cir. 1982). "The same principles apply to the waiver of work product protection." *E.I. Dupont de Nemours & Co. v. Kolon Indus., Inc.*, 269 F.R.D. 600, 605 (E.D. Va. 2010).

Courts recognize two categories of work product: fact work product and opinion work product. *In re Grand Jury Proceedings, Thursday Special Grand Jury Sept. Term, 1991*, 33 F.3d 342, 348 (4th Cir. 1994) (citing *In re John Doe*, 662 F.2d 1073, 1078-80 (4th Cir. 1981)). Opinion work product – which contains "the mental impressions, conclusions, opinions, or legal theories of a party's attorney or other representative concerning the litigation" – is inviolate. Fed. R. Civ. P. 26(b)(3)(B); *In re Doe*, 662 F.2d at 1080. Litigants, however, cannot shield underlying facts from disclosure under the work product doctrine by communicating them to an attorney or having

an attorney direct the fact investigation. *In re Zetia (Ezetimibe) Antitrust Litig.*, No. 2:18MD2836, 2019 WL 6122012, at *3 (E.D. Va. July 16, 2019) (citing *Upjohn Co. v. United States*, 449 U.S. 383, 395 (1981)).

Work product can also be discoverable where "the party shows that it has substantial need for the materials to prepare its case and cannot, without undue hardship, obtain their substantial equivalent by other means." Fed. R. Civ. P. at 26(b)(3)(A)(ii). When fact work product is at issue, courts consider "the document's relevance and importance to the issues in the litigation and the unavailability of the facts in the documents from other sources." *Nat'l Union Fire Ins.*, 967 F.2d at 985.

B. Attorney-Client Privilege

Virginia law applies to the invocation of attorney-client privilege in this case. Fed. R. Evid. 501. Under Virginia law, "confidential communications between an attorney and his or her client made in the course of that relationship and concerning the subject matter of the attorney's representation are privileged from disclosure." *Walton v. Mid-Atl. Spine Specialists, P.C.*, 694 S.E.2d 545, 549 (Va. 2010). "Nevertheless, the privilege is an exception to the general duty to disclose, is an obstacle to investigation of the truth, and should be strictly construed." *Commonwealth v. Edwards*, 370 S.E.2d 296, 301 (Va. 1988). Not all communications with attorneys are privileged, however; only communications made for the purpose of seeking or providing legal advice are subject to the protection. *Virginia Elec. & Power Co. v. Westmoreland-LG & E Partners*, 526 S.E.2d 750, 755 (Va. 2000) ("The attorney-client privilege does not attach to a document merely because a client delivers it to his attorney"); *Chevalier-Seawell v. Mangum*, 90 Va. Cir. 420, at *6 (2015) ("[W]here a communication neither requests nor expresses legal advice, but rather involves the soliciting or giving of business advice, it is not protected by the privilege.") (quoting *Adair v. EQT Prod. Co.*, 285 F.R.D. 376, 380 (W.D.Va. 2012)).

"The proponent of the privilege has the burden to establish that the attorney-client relationship existed, that the communication under consideration is privileged, and that the privilege was not waived." *Walton*, 694 S.E.2d at 549. "The privilege attaches to communications of the client made to the attorney's agents . . . when such agent's services are indispensable to the attorney's effective representation of the client." *Edwards*, 370 S.E.2d at 301. But the burden of establishing "indispensability" is on the party claiming privilege. *Via v. Commonwealth*, 590 S.E.2d 583, 595 (Va. 2004).

Underlying facts, however, are not protected from disclosure under the attorney-client privilege merely because they were conveyed by the client to the attorney. *Indus. Chemicals, Inc. v. Rehrig Int'l, Inc.*, 2 Va. Cir. 147, at *1 (1983) (citing *Upjohn*, 449 U.S. at 383).

ARGUMENT

A. Courts in other data breach cases – including in this District – regularly order defendants to produce Mandiant reports because Mandiant serves a business purpose.

Mandiant is a cyber security consultant that provides data security services to its clients, including breach response, security enhancement, security transformation, and security assessment.[3] Mandiant markets itself as helping "organizations effectively . . . respond to threats and reduce overall impact of *business risk* – before, during and after an incident."[4] Mandiant does not market itself as a consulting or testifying expert for litigation.[5] Due to its prominence in providing business-oriented data security services, Mandiant has become a repeat player in data

[3] FireEye Mandiant Website, available at https://www.fireeye.com/services.html (last visited April 24, 2020).
[4] *Id.* (emphasis added).
[5] *Id.*

breach litigation as the third-party entity who often investigates, or in some cases, discovers the breach and then helps the breached entity patch up its security.[6]

In some cases, defendants recognize that the highly-technical, forensic report prepared by Mandiant for business purposes should be produced and do so without contending its privilege. *See In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617-LHK, 2016 WL 3029783, at *3 (N.D. Cal. May 27, 2016) ("[A]fter learning of the cyberattacks, Anthem retained Mandiant, a cybersecurity company, 'to assist in assessing and responding to the Anthem Data Breach and to assist in developing security protocols for Anthem.' Mandiant's work culminated in the production of an Intrusion Investigation Report ('Mandiant Report'), which Mandiant provided to Anthem in July 2015[,]" and which was subsequently provided to plaintiffs); *Fero v. Excellus Health Plan, Inc.*, 304 F. Supp. 3d 333, 342 (W.D.N.Y. 2018) (providing Mandiant Report to plaintiffs and their expert early in the case).

But in other cases, in order to prevent the disclosure of Mandiant's forensic analysis and remedial recommendations, and to obfuscate key liability facts, counsel for breached defendants have tried to shield these key documents from production by claiming privilege or protection under the work product doctrine. In most cases, defendants have been unsuccessful.

[6] *See S. Indep. Bank v. Fred's, Inc*., No. 2:15-CV-799-WKW, 2019 WL 1179396, at *3 (M.D. Ala. Mar. 13, 2019) (stating that Fred's, a general goods retailer, "hired cybersecurity firm Mandiant to do a forensic investigation of the data breach and issue a report" which appears to have been produced in that case); *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1310 (N.D. Ga. 2019) ("Equifax also hired cybersecurity firm Mandiant to investigate the suspicious activity."); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 313 F. Supp. 3d 1113, 1121 (N.D. Cal. 2018) ("Yahoo also hired security firms who identified problems with Yahoo's systems. For example, in 2012, Yahoo retained Mandiant, an outside cybersecurity firm, to perform a threat assessment; Mandiant's subsequent report detailed issues with Yahoo's security and attack groups in Yahoo's systems.").

For example, as described *supra*, in a recent data breach case in this District, Judge Nachmanoff rejected the defendants' assertion of privilege where Mandiant had been retained for similar incident response services several years *before* the data breach occurred and litigation anticipated. *In re Dominion National,* 2019 WL 7592343 at *4. Even though after the breach was discovered the defendant's *counsel* engaged Mandiant, the Court explained that the defendants had "done little to show 'that Mandiant changed the nature of its investigations at the instruction of outside counsel and that Mandiant's scope of work and purpose became different in anticipation of litigation.'" *Id.* (*quoting In re Premera,* 296 F. Supp. 3d at 1246). Therefore, the Court found that the "driving force" behind the Mandiant Report "was not litigation, but business purposes." *Id.* So too here.

Similarly, in the *Premera Blue Cross Customer Data Security Breach Litigation,* Judge Simon in the District of Oregon ordered Premera Blue Cross to produce the Mandiant Report and related non-privileged or work-product communications. In *Premera,* Mandiant was initially hired by Premera, but prior to the issuance of its report, entered into an amended agreement with Premera's counsel that shifted supervisory authority from Premera to counsel. *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 296 F. Supp. 3d 1230, 1245 (D. Or. 2017). Premera objected to production claiming that "Mandiant [was] the equivalent of a private investigator or other investigative resource hired by an attorney to conduct an investigation on behalf of an attorney, and thus that Mandiant's work [was] privileged and protected as work-product." *Id.* The Court rejected this theory citing the fact that the only change from Mandiant's initial obligations under its agreement with Premera and the amended obligations with counsel was that Mandiant was directed to mark its communications as "privileged," "work-product," or "on request of counsel." *Id.* Further, Judge Simon expressly found that Premera's investigation into the cause of

the breach was a "necessary business function regardless of litigation" that was "conducted primarily for a business purpose." *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 329 F.R.D. 656, 666 (D. Or. 2019).[7] The same conclusion is necessary here.

B. The Mandiant Report is not work product.

Plaintiffs do not know exactly when, after the Breach, Mandiant was purportedly retained by Capital One's counsel to perform [redacted] But even though Mandiant was facially hired by Capital One's counsel, it makes no difference: Mandiant's investigation and resulting report(s) are not work product. [redacted]

The investigation and resulting reports fail the "because of" test required in assessing work product claims under any plausible analysis of the facts and circumstances. *See RLI Ins.*, 477 F. Supp. 2d at 748 (holding investigation not work product when there was no evidence that review would have been different had party "been conducting a conventional investigation"). Determining what caused the breach and identifying efforts necessary to remediate the security failures that caused it in the first instance *and* prevented it from being discovered for four months is not a legal

[7] Capital One's situation is distinguishable from cases Plaintiffs anticipate Capital One will rely on, such as *In re Experian Data Breach Litig.*, No. SACV1501592AGDFMX, 2017 WL 4325583 (C.D. Cal. May 18, 2017). In *Experian* – which was decided under slightly different Ninth Circuit standards – Experian retained Jones Day immediately after discovering the breach and Jones Day in turn hired Mandiant to conduct an investigation to assist it in providing legal advice. *Id.* at *2. But in *Experian* the Court determined that "Mandiant's previous work for Experian was separate from the work it did for Experian regarding this particular data breach." *Id.* at *3. That is not the case here. [redacted]

investigation; it is a factual investigation. This investigation would have necessarily been conducted in the absence of litigation or Capital One retaining counsel. While Capital One's counsel may have simultaneously benefited from the investigation and used it to provide legal advice to their clients, Capital One cannot credibly claim that it would not have conducted the investigation but for the anticipated threat of litigation; particularly when, [redacted]

To the contrary, Capital One, as a regulated banking entity, is required under federal law to ensure the adequacy of its data security. *See, e.g.*, Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6801(a)-(b) (requiring financial institutions to "protect the security and confidentiality of [] customers' nonpublic personal information"). Capital One was therefore obligated to investigate the breach, its cause, and identify and implement appropriate remedial measures to protect its customers' personal information, even in the absence of prospective litigation. *See Collins v. Mullins*, 170 F.R.D. 132, 135 (W.D. Va. 1996) (holding that Sheriff department's investigation of internal misconduct was not protected by work product privilege where internal policies required the investigation even though Sheriff's office was aware that litigation arising from the misconduct was likely).

Further, documents in Capital One's initial document productions show that [redacted] *See* Ex. 4, CAPITALONE_MDL_000115137 ([redacted]); Ex.

5, CAPITALONE_MDL_000100994, at -100999 and -101001 ([redacted]). Indeed, Capital One's outside auditors, Ernst & Young ("EY"), [redacted] Ex. 6, CAPITALONE_MDL_000247842 ([redacted]) (emphasis in original). These facts show that Capital One had numerous, overarching business purposes for which it needed Mandiant's investigation, and that the primary purpose of the investigation was not litigation.

In addition to its non-litigation obligations to conduct an investigation, there is other strong evidence that [redacted] First and foremost, [redacted] Ex. 1, Master Services Agreement. [redacted] Ex. 2, Statement of Work. Pursuant to the Statement of Work, [redacted] *Id.* at Section 2.1. So that Capital One [redacted] *Id.* at Section 4.

Moreover, Capital One's initial document production confirms [redacted] For example, [redacted] Ex. 7, CAPITALONE_MDL_000248419, at -248421. Critically, [redacted] Ex. 3, CAPITALONE_MDL_000185309, at 319. And [redacted] Ex. [ ], CAPITALONE_MDL_000251578.

In July 2019, when Capital One discovered it had experienced the Data Breach, it turned to Mandiant [redacted] In fact, as evidenced by communications after Capital One discovered the Data Breach, [redacted] *See* Ex. 9, CAPITALONE_MDL_000097216 ([redacted]); *see also* Ex. 2 ([redacted]).

That Capital One's outside counsel then purportedly engaged[8] Mandiant to conduct [redacted] shows that only a veneer of privilege – not actual privilege – exists. [redacted] and that the resultant report ([redacted]) and communications related to its investigation are not work product. Indeed, the Mandiant Report, which is a forensic report, was almost certainly prepared in essentially the same form that it would have been absent litigation. *See RLI Ins.*, 477 F. Supp. 2d at 748 (explaining the principal inquiry is whether the document "would not have been prepared in substantially similar form *but for* the prospect of that litigation.") (quoting *United States v. Adlman*, 134 F.3d 1194, 1195 (2d Cir. 1998)) (emphasis in original).

For all of the above-stated reasons, the Court should find the Mandiant Report is not work product.

C. The Mandiant Report is not protected by the attorney-client privilege.

Similarly, the Mandiant report is not protected by the Attorney-Client privilege. Mandiant is a data security and incident response consultant employed to "reduce overall impact of business risk" – not a legal expert. Mandiant's investigation could not have, therefore, been performed using any legal expertise nor would Mandiant itself have provided legal advice to Capital One. *Cf. In re Allen*, 106 F.3d 582, 602–03 (4th Cir. 1997) (finding attorney hired to conduct factual investigation was "retained to conduct an investigation using her legal expertise" but recognizing that no privilege attaches when investigation is performed in a capacity other than as a lawyer). Virginia

[8] Despite requesting all agreements and statements of work associated with Mandiant, Plaintiffs have not been provided a copy of the purported agreement between Debevoise and Mandiant, nor does the agreement appear on Capital One's privilege log. *See* Ex. 14, Feb. 5, 2020 Email from J. Dent to R. Solomon.

law is clear that "attorney-client privilege does not attach to a document merely because a client delivers it to his attorney." *Virginia Elec.*, 526 S.E.2d at 755.

In order for attorney-client privilege to attach, Capital One bears the burden of proving that the Report was prepared with the intention of securing legal advice on its contents. *Id.* Capital One cannot make that requisite showing, however, because [redacted] *See, e.g.*, Ex. 6, CAPITALONE_MDL_000247842 ([redacted]) (emphasis in original); Ex. 10, CAPITALONE_MDL_000232681 ([redacted]). Accordingly, it is not privileged.

Although Capital One's counsel may have provided legal services utilizing the report, the report was prepared – and would have been prepared in the absence of litigation – to memorialize Mandiant's factual investigation. *See In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 329 F.R.D. at 665 ("The Court previously found that third parties performing general remediation efforts, even if hired by counsel, are performing a business function. Accordingly, the fact that a third-party vendor prepared a remediation-related document and sent it to outside counsel is insufficient to designate that document as subject to the attorney-client privilege or work-product protection.") (internal citation omitted).

D. Even if the Mandiant Report was protected by work product or attorney-client privilege, those privileges have been waived.

Finally, because Capital One disclosed some of Mandiant's findings and distributed the report and findings to third parties, it has waived its privilege claim to the Mandiant Report. Importantly, the burden is on Capital One to prove that it has *not* waived any privilege. *Walton*, 694 S.E.2d at 549. A privilege holder may waive privilege when "'the privilege holder's conduct

makes it unfair to allow subsequent assertion of the privilege.'" *Id.* at 552 (quoting *United States v. Yerardi*, 192 F.3d 14, 18 (1st Cir. 1999)).

Although Plaintiffs do not yet know who received the Mandiant Report, despite requesting such information months ago on February 5, 2020,[9] Capital One's documents produced to date show that [redacted] First, Capital One's documents [redacted] *See* Ex. 10, CAPITALONE_MDL_000232681 ([redacted]);[10] *see also E.I. Dupont*, 269 F.R.D at 605 (privilege over a document may be waived when a document is shared with a governmental agency that is "in a position adversarial to the disclosing party"). Second, Capital One has [redacted] *See* Ex. 6, CAPITALONE_MDL_000247842 ([redacted]). Third, it appears from at least one document that [redacted][11] [redacted] *See* Ex. 12,

[9] *See* Ex. 14, Feb. 5, 2020 Email from J. Dent to R. Solomon.

[10] Although [redacted] Ex. 11, CAPITALONE_MDL_000172998 ([redacted]).

[11] *See* LinkedIn of Danielle Dietz, Managing Vice President of Investor Relations, available at https://www.linkedin.com/in/danielle-dietz-8b70b98/ (last visited April 24, 2020).

CAPITALONE_MDL_000086014, at -86016. These disclosures of Mandiant's conclusions and the Report itself constitute waiver, if the report ever was privileged.

Moreover, Capital One has placed *at least* two of the major findings of the Mandiant Report at issue in this litigation, resulting in subject matter waiver. First, Capital One has represented to both Plaintiffs and the public that after the Data Breach it "immediately fixed the issue."[12] Capital One has further [redacted] Ex. 13, Amended Interrogatory Answers at Answer 12. Whether Capital One actually "fixed the issue" as it has represented and remediated the issues that led to the Data Breach are very much in dispute, and are addressed in the Mandiant Report. If Mandiant recommended other remedial actions Capital One has not taken, Plaintiffs are entitled to know.

Even more critically, Capital One has placed at issue whether other hackers accessed the data involved in this Data Breach, given the fact that the instructions for accessing the data had been posted publicly on GitHub for many months. Compl. ¶¶ 63-64, 83. In its Interrogatory Answers, Capital One represented that [redacted] Ex. 13, Amended Interrogatory Answer 6. Whether other hackers performed the steps publicly posted on GitHub – or whether Capital One can even know whether such steps were performed – is information that would almost certainly be included in the Mandiant Report. Because Capital One has placed this information at issue, it has waived the privilege. *See United States v. Jones*, 696 F.2d 1069, 1072 (4th Cir. 1982) ("Selective disclosure for tactical purposes waives the privilege.").

[12] Information on the Capital One Cyber Incident, available at https://www.capitalone.com/facts2019/ (last visited April 24, 2020).

E. Communications regarding Mandiant's investigation, findings, and recommendations are not work product or privileged.

As Mandiant's investigation and report are not privileged or work product, Plaintiffs also seek non-privileged, non-work product communications (1) between Mandiant and Capital One employees regarding the breach and remediation, (2) between Capital One employees and third-parties discussing the Mandiant report and its conclusions, and (3) between multiple Capital One employees discussing the Mandiant report, its conclusions and recommendations, and efforts to implement proposed remediation measures. Importantly, Plaintiffs do not seek communications between Capital One and counsel soliciting or providing legal advice, or Mandiant and counsel conveying either's thoughts, opinions, impressions, or legal conclusions about this litigation. However, Plaintiffs *do* seek communications that may have the veneer of containing attorney-client privileged content simply because, for example, counsel was cc'd or bcc'd on an e-mail chain, but were not created for the purpose of securing legal advice or in response to this litigation. The communications sought are discoverable and not privileged.

As discussed *supra*, Judge Nachmanoff found that because the Mandiant Report was not work product, the "associated communications" in the Mandiant investigation were not privileged. *In re: Dominion Dental Servs. USA, Inc. Data Breach Litig.*, 2019 WL 7592343, at *3. Judge Simon in the *Premera* matter likewise addressed this issue. He held that when employees are discussing a document prepared by a third-party vendor, the fact that an attorney is on the email does not necessarily render the communication or the document itself privileged. *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 329 F.R.D. at 667 (concluding that Mandiant was providing business advice not protected by privilege). Instead, the "email must independently qualify as privileged" and is "only privileged if the attorney is being asked to provide legal input and advice." *Id*. "Similarly, if [] employees generally are discussing factual information relating

to a third-party vendors' services with counsel, and not requesting or receiving legal advice or providing facts to the attorney to provide legal services, the email would not be privileged." *Id.*

Capital One's attempts to withhold relevant communications regarding the Data Breach, the reason for Capital One's failure to timely discover it, and remediation far exceed the bounds of the attorney-client privilege. The underlying facts that Mandiant's investigation discovered are undoubtedly not privileged and Capital One's consideration of Mandiant's conclusions and recommendations is a business function, not a request for or provision of legal advice. Further, because Capital One would have needed to investigate and correct its data security deficiencies even in the absence of litigation, none of these communications can qualify as work product. The Court should therefore order Capital One to produce all such communications.

F. In the alternative, Plaintiffs can establish substantial need and undue hardship.

Even if the Court concludes that the Mandiant Report is work product, it should nevertheless compel Capital One to produce it under the exception in Rule 26(b)(3)(A)(ii). Plaintiffs have a substantial need for the Report and it will be impossible or unduly difficult for Plaintiffs to obtain the same information through other means.

Plaintiffs have a substantial need for the Mandiant Report. It outlines, in forensic detail, all of Capital One's data security failures that lead to or contributed to both the Data Breach itself and Capital One's failure to discover the Data Breach for four months. It is a crucial liability document that will enable Plaintiffs to prosecute their case more efficiently. Indeed, production of the Report will necessarily streamline the discovery process, which will benefit Capital One as well. To obtain the same information contained in the Mandiant Report will impose undue hardship on Plaintiffs. Plaintiffs will have to obtain and search through thousands of documents and communications – many of which may have no relevance to the Breach at all – to piece together and identify these deficiencies that Capital One already uncovered and for which they took several months to explore.

Capital One may point to the fact that it is providing documents such as event logs and network diagrams to Plaintiffs. But the provision of such limited technical documents is insufficient for several reasons. Unlike Mandiant, Plaintiffs will not have the ability to question Capital One cyber security and infrastructure employees at will. They will be confined to limited depositions, the preparation for which will require Plaintiffs to have already reached their conclusions regarding the cause of the breach and Capital One's failure to timely discover it. If Plaintiffs had a year to conduct discovery and increased access to interview employees, that might be feasible, but they do not. Further, Plaintiffs have brought claims for injunctive relief and are entitled to know the entire universe of remediation recommendations that were presented to Capital One. If Mandiant made deficiency findings that Capital One has not corrected or remediation recommendations that it has not implemented, this information can only be discovered – and more importantly confirmed – by actually reviewing Mandiant's Report.

CONCLUSION

For all the reasons set forth above, Plaintiffs request that the Court issue an order compelling Capital One to produce (1) any and all Mandiant reports regarding the Data Breach, the reason for its duration, and remediation, (2) communications between Mandiant and Capital One employees regarding its factual conclusions and remediation; and (3) communications between Capital One employees discussing the Mandiant report, its conclusions and recommended remediation measures.

Dated: April 24, 2020.

Respectfully Submitted,

/s/ Steven T. Webster

Steven T. Webster (VSB No. 31975)
WEBSTER BOOK LLP
300 N. Washington Street, Suite 404
Alexandria, Virginia 22314
Tel: (888) 987-9991

swebster@websterbook.com

Plaintiffs' Local Counsel

Norman E. Siegel
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, MO 64112
Tel: (816) 714-7100
siegel@stuevesiegel.com

Karen Hanson Riebel
LOCKRIDGE GRINDAL NAUEN, P.L.L.P
100 Washington Avenue South, Suite 200
Minneapolis, MN 55401
Tel: (612) 339-6900
khriebel@locklaw.com

John A. Yanchunis
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel: (813) 223-5505
jyanchunis@ForThePeople.com

Plaintiffs' Co-Lead Counsel

CERTIFICATE OF SERVICE

I hereby certify that on April 24, 2020, I electronically filed the foregoing document with the Clerk of the Court using the CM/ECF system, which will send notice of electronic filing to all counsel of record.

/s/ Steven T. Webster
Steven T. Webster (VSB No. 31975)
WEBSTER BOOK LLP